ZKTeco ZKAccess Professional 3.5.3 Insecure File Permissions

2016.08.31

Credit: **Gjoko 'LiquidWorm' Krstic (https://cxsecurity.com/author/Gjoko+%26%23039%3BLiquidWorm%26%23039%3B+Krstic/1/)**

Risk: **Low** | Local: **Yes** | Remote: **No**

CVE: **N/A** | CWE: **N/A**

ZKTeco ZKAccess Professional 3.5.3 Insecure File Permissions

Vendor: ZKTeco Inc. | Xiamen ZKTeco Biometric Identification Technology Co.,ltd
Product web page: http://www.zkteco.com
Affected version: 3.5.3 (Build 0005)

Summary: ZKAccess 3.5 is a desktop software which is suitable for small and medium businesses application. Compatible with all ZKAccess standalone reader controllers, the software can simultaneously manage access control and generate attendance report. The brand new flat GUI design and humanized structure of new ZKAccess 3.5 will make your daily management more pleasant and convenient.

Desc: ZKAccess suffers from an elevation of privileges vulnerability which can be used by a simple authenticated user that can change the executable file with a binary of choice. The vulnerability exist due to the improper permissions, with the 'M' flag (Modify) for 'Authenticated Users'
group.

```
Tested on: Microsoft Windows 7 Ultimate SP1 (EN)
           Microsoft Windows 7 Professional SP1 (EN)


Vulnerability discovered by Gjoko 'LiquidWorm' Krstic
                            @zeroscience


Advisory ID: ZSL-2016-5361
Advisory URL: http://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5
361.php


18.07.2016

--


C:ZKTeco>icacls ZKAccess3.5
ZKAccess3.5 BUILTINAdministrators:(I)(F)
            BUILTINAdministrators:(I)(OI)(CI)(IO)(F)
            NT AUTHORITYSYSTEM:(I)(F)
            NT AUTHORITYSYSTEM:(I)(OI)(CI)(IO)(F)
            BUILTINUsers:(I)(OI)(CI)(RX)
            NT AUTHORITYAuthenticated Users:(I)(M)
            NT AUTHORITYAuthenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files
```

References:

http://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5361.php

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)